On the Complexity of Fair Coin Flipping

Working draft: do not distribute

Iftach Haitner*† Nikolaos Makriyannis‡‡ Eran Omri§

April 5, 2018

Abstract

In their breakthrough result, Moran et al. [Journal of Cryptology '16] show how to construct an r-round two-party coin-flipping with bias $\Theta(1/r)$, for any $r \in \mathbb{N}$. This improves over the $\Theta(1/\sqrt{r})$ protocol of Awerbuch et al. [Manuscript '85], and matches the lower bound of Cleve [STOC '86]. The protocol of [18], however, uses oblivious transfer, to be compared with the protocol of [3] that can be based on any one-way function. An intriguing open question is whether oblivious transfer, or more generally "public-key primitives", is required for an $o(1/\sqrt{r})$-bias coin flipping. The question was partially answered in the black-box settings by Dachman-Soled et al. [11] [TCC '11] and Dachman-Soled et al. [12] [TCC '14], who showd that *restricted* types of fully black-box reductions cannot established such $o(1/\sqrt{r})$-bias coin-flipping protocols from one-way functions.

We make progress towards answering the above question, showing that for any (constant) $r \in \mathbb{N}$, an $o(1/\sqrt{r})$-bias coin-flipping protocol can be use to construct an infinitely-often key-agreement protocol. Our reduction is non black-box, and makes a novel use of the recent dichotomy for two-party protocols of Haitner et al. [15] to facilitate for the two party case the recent attack of Beimel et al. [5] on many-party coin-flipping protocols.

*School of Computer Science, Tel Aviv University. E-mail: iftachh@cs.tau.ac.il. Member of the Israeli Center of Research Excellence in Algorithms (ICORE) and the Check Point Institute for Information Security.

†Research supported by ERC starting grant 638121.

‡School of Computer Science, Tel Aviv University. E-mail: n.makriyannis@gmail.com

§Department of Computer Science, Ariel University. E-mail: omrier@ariel.ac.il. Research supported by ISF grant 152/17.

Contents

1 Introduction **1**
- 1.1 Our Results . . . 1
- 1.2 Our Technique . . . 1
- 1.3 Related Work . . . 5

2 Preliminaries **6**
- 2.1 Notation . . . 6
- 2.2 Protocols . . . 6
- 2.3 Martingales . . . 7

3 Fair Coin-Flipping to Key Agreement **7**
- 3.1 Game Values are Efficiently Approximateable . . . 12
- 3.2 Forecasted Backup Values are Close to Game Values . . . 13
- 3.3 Independence of Attack Decision . . . 15

1 Introduction

In a two-party coin-flipping protocol, introduced by Blum [7], the parties wish to output a common (close to) uniform bit, even though one of the parties may be corrupted and try to bias the output. Slightly more formally, a (fair) coin-flipping protocol should satisfy the following two properties: first, when both parties behave honestly (i.e., follow the prescribed protocol), they both output the *same* bit. Second, the output of an honest party should always be an (almost) unbiased bit – even if the other party is corrupted (i.e., arbitrarily deviates from the protocol) (i.e., its distribution should be close to being uniform over $\{0,1\}$). We emphasize that the above notion requires an honest party to *always* output a bit, regardless of what the corrupted party does, and in particular it is not allowed to abort if a cheat was detected.[1] Coin-flipping is a fundamental primitive with numerous applications, and thus lower bounds on coin-flipping protocols imply the analogous bounds on many basic cryptographic primitives including other input-less primitives and secure computation of functions that take input (e.g., XOR).

In his seminal work, Cleve [9] showed that for *any* efficient two-party r-round coin-flipping protocol, there exists an efficient adversarial strategy that biases the output of the honest party by $\Theta(1/r)$. The above lower bound on coin-flipping protocols was met for the two-party case by Moran, Naor, and Segev [18] improving over the $\Theta(n/\sqrt{r})$-bias achieved by the majority protocol of Awerbuch, Blum, Chor, Goldwasser, and Micali [3]. The protocol of [18], however, uses oblivious transfer, to be compared with the protocol of [3] that can be based on any one-way function. An intriguing open question is whether oblivious transfer, or more generally "public-key primitives", is required for an $o(1/\sqrt{r})$-bias coin-flipping. The question was partially answered in the black-box settings by Dachman-Soled et al. [11] and Dachman-Soled et al. [12], who showed that *restricted* types of fully black-box reductions cannot established such $o(1/\sqrt{r})$-bias coin-flipping protocols from one-way functions.

1.1 Our Results

Our main result is that constant-round coin-flipping protocols with better bias than that of the majority protocol of [2] implies the existence of infinitely-often key-agreement.

Theorem 1.1 (Main result, informal)**.** *For any (constant) $r \in \mathbb{N}$, an $o(1/\sqrt{r})$-bias r-round coin-flipping protocol can be used to construct an infinitely-often key-agreement protocol*

As in [9, 11, 12], our result extends via a simple reduction to general multiparty coin-flipping protocols (with more than two-parties) without an honest majority. Our reduction is non black-box, and makes a novel use of the recent dichotomy for two-party protocols of Haitner et al. [15] to enable for the two party case the recent attack of Beimel et al. [5] on many-party coin-flipping protocols.

1.2 Our Technique

Let $\Pi = (\mathsf{A}, \mathsf{B})$ be an r-round two-party coin-flipping protocol. We show that the inexistence of an infinitely-often (io-)key-agreement protocol, yields an efficient $\Theta(1/\sqrt{r})$-bias attack on Π.

We start by describing the $1/\sqrt{r}$-bias inefficient attack of Cleve and Impagliazzo [10], and the approach of Beimel et al. [5] towards making this attack efficient. We then explain how to use

[1] Such protocols are typically addressed as having *guaranteed output delivery*, or, abusing terminology, as *fair*.

the recent results by Haitner et al. [15] to mount an efficient attack assuming io-key-agreement protocols do not exist .

1.2.1 Cleve and Impagliazzo's Inefficient Attack

Let $M_1, \ldots, M_r$ denote the messages in a random execution of Π and let out denote the (always common) output of the parties in a random honest execution of the protocol. Let $X_i = \mathbf{E}[\mathsf{out} \mid T_i]$. Namely, X_i is the expected outcome of the protocol given $T_i = M_1, \ldots, M_i$. It is easy to see that $X_1, \ldots, X_r$ is a martingale sequence. That is, $\mathbf{E}[X_i \mid X_{<i}] = X_{i-1}$ for every i. Since the parties in an honest execution of Π output a uniform bit, it holds that $X_0 = \Pr[\mathsf{out} = 1] = 1/2$ and $X_r \in \{0, 1\}$. Cleve and Impagliazzo [10] (see Beimel et al. [5] for an alternative simpler proof) prove that for such a sequence it holds that (omitting absolute values and constant factors)

$$\text{Jump:} \qquad \Pr\left[\exists i \in [r] \colon X_i - X_{i-1} \geq 1/\sqrt{r}\right] \geq 1/2 \tag{1}$$

The *backup* value Z_i^{P} denotes the output of party P if the other aborts prematurely *after* the i^{th} message was sent. In particular, Z_r^{P} denotes the final output of P (no abort occurred). Note that, by definition, $Z_r^{\mathsf{A}} = Z_r^{\mathsf{B}}$. We assume that

$$\text{Backup values approximate outcome:} \quad \Pr\left[\exists i \in [r] \colon \left|X_i - \mathbf{E}\left[Z_i^{\mathsf{P}} \mid T_i\right]\right| \geq 1/2\sqrt{r}\right] \leq 1/4 \tag{2}$$

for both $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$. Otherwise, without loss of generality, the (possibly inefficient) adversary that controls A and aborts after M_i was sent if $X_i - \mathbf{E}\left[Z_i^{\mathsf{B}} \mid T_i\right] \geq 1/\sqrt{r}$, biases the output of B towards zero by $\Theta(1/\sqrt{r})$, and we are done. Finally, the coins of the parties are *independent* conditioned on the transcript. Thus, if for example party A sends the $(i+1)$ message, it holds that

$$\text{Independence:} \qquad \mathbf{E}\left[Z_i^{\mathsf{B}} \mid T_i\right] = \mathbf{E}\left[Z_i^{\mathsf{B}} \mid T_{i+1}\right] \tag{3}$$

Combining the above observations yields that without loss of generality:

$$\Pr\left[\exists i \in [r] \colon \mathsf{A} \text{ sends the } i^{\text{th}} \text{ message} \wedge X_i - \mathbf{E}\left[Z_{i-1}^{\mathsf{B}} \mid T_i\right] \geq 1/2\sqrt{r}\right] \geq 1/8 \tag{4}$$

Equation (4) implies the following (possibly inefficient) attack for a corrupted party A biasing B's output towards zero: before sending the i^{th} message M_i, party A aborts if $X_i - \mathbf{E}\left[Z_{i-1}^{\mathsf{B}} \mid T_i\right] \geq 1/2\sqrt{r}$. By Equation (4), this attack biases B output towards zero by $\Omega(1/2\sqrt{r})$.

The clear limitation of the above attack is that, assuming one-way functions, the value of $X_i = \mathbf{E}[\mathsf{out} \mid T_i = t]$ and of $\mathbf{E}\left[Z_i^{\mathsf{P}} \mid T_i = t\right]$ might *not* be efficiently computable (as a function of t). For instance, assume that the first two messages contain commitments to the parties' randomness.

Facing this difficulty, Beimel et al. [5] associate a different sequence of random variables $Y_1, \ldots, Y_r$ with the protocol's execution, where each of the Y_i has a *polynomial* size support. They then define the martingale sequence $X_i = \mathbf{E}[\mathsf{out} \mid Y_{\leq i}]$. It follows that for constant-round protocols the value of X_i is only a function of a constant size string, and thus it is efficiently computable. Beimel et al. [5] exploit this observation to present an efficient $\widetilde{\Omega}(1/\sqrt{r})$-attack on coin-tossing protocols for *many* parties. In the following, we show how to emulate the approach of Beimel et al. [5] for two-party protocols, using the dichotomy of Haitner et al. [15].

1.2.2 Inexistence of Key-Agreement Implies an Efficient Attack

Let U_p denote the Bernoulli random variable taking the value 1 with probability p, and let $P \overset{\text{C}}{\approx}_\rho Q$ stand for Q and P are ρ-computationally indistinguishability (i.e., an efficient distinguisher cannot tell P from Q with advantage better than ρ). We are using two results by Haitner et al. [15]. The first one given below holds fo any efficient protocol.

Theorem 1.2 (Haitner et al. [15]'s forecaster, informal)**.** *Let $\Delta = (\mathsf{A}, \mathsf{B})$ be an efficient single-bit output (each party outputs a bit) two-party protocol. Then for any constant $\rho > 0$ there exists a* PPT *algorithm (forecaster) F mapping transcripts of Δ into (the binary description of) pairs in $[0,1] \times [0,1]$, such that the following holds: let (X, Y, T) be the parties outputs and transcript in a random execution of Δ then*[2]

- $(X, T) \overset{\text{C}}{\approx}_\rho (U_{p^{\mathsf{A}}}, T)_{(p^{\mathsf{A}},\cdot)\leftarrow\mathsf{F}(T)}$, *and*
- $(Y, T) \overset{\text{C}}{\approx}_\rho (U_{p^{\mathsf{B}}}, T)_{(\cdot,p^{\mathsf{B}})\leftarrow\mathsf{F}(T)}$.

Namely, given the transcript, F forecasts the output distribution of each of the parties in a way that is computationally distinguishable from the real value. In the following we assume for simplicity that the guaranteed forecaster is deterministic and assume without loss of generality that it has *constant* output length (indeed, since we only care about constant, $1/r$, indistinguishability, we can chop its output to the first $\log r$ bits).

Consider the $(r+1)$-round protocol $\widetilde{\pi} = (\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}})$, defined by $\widetilde{\mathsf{A}}$ sending a random $i \in [r]$ to $\widetilde{\mathsf{B}}$ as the first message, and then the parties interact in a random execution of Π for i rounds. At the end of the execution, the parties output their i^{th} backup values z_i^{A} and z_i^{B} and halt. Let $\widetilde{\mathsf{F}}$ be the forecaster for $\widetilde{\pi}$ guaranteed by Theorem 1.2 for $\rho = 1/r^2$ (note that ρ is indeed constant). A simple averaging argument yields that

$$(Z_i^{\mathsf{P}}, T_i) \overset{\text{C}}{\approx}_{1/r} (U_{p^{\mathsf{P}}}, T_i)_{(p^{\mathsf{A}},p^{\mathsf{B}})\leftarrow\widetilde{\mathsf{F}}(i,T_{\leq i})}, \tag{5}$$

for both $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ and every $i \in [r]$. Namely, $\widetilde{\mathsf{F}}$ is a good forecaster for the partial transcripts of Π.

Let $M_1, \ldots, M_r$ denote the messages in a random execution of Π and let out denote the output of the parties in Π. Let $Y_i = \left(Y_i^{\mathsf{A}}, Y_i^{\mathsf{B}}\right) = \widetilde{\mathsf{F}}(i, T_i)$ and let $X_i = \mathbf{E}\left[\mathsf{out} \mid Y_{\leq i}\right]$. It is easy to see that $X_1, \ldots, X_r$ is a martingale sequence and that $X_0 = 1/2$. Without loss of generality, we assume that the last message of Π contains the common output. It follows from Equation (5) that $Y_r \approx (\mathsf{out}, \mathsf{out}) \in \{(0,0), (1,1)\}$ (otherwise, it will be very easy to distinguish the emulated outputs from the real ones, given M_r). Hence, similarly to Section 1.2.1, it holds that

$$\text{Jump:} \qquad \Pr\left[\exists i \in [r] \colon X_i - X_{i-1} \geq 1/\sqrt{r}\right] \geq 1/2 \tag{6}$$

Since Y_i has constant size support and since Π is constant round, it follows that X_i is efficiently computable from T_i.[3]

[2] Actually, the following only holds for infinitely many lengths of the security parameter, but we ignore this subtlety for the current discussion.

[3] In the spirit of Beimel et al. [5], we could have modified the definition of the X_i's to make them efficiently computable even for non constant-round protocols. The idea is to define $X_i = \mathbf{E}\left[\mathsf{out} \mid Y_i, X_{i-1}\right]$. While the resulting sequence might not be a martingale, [5] proves that a $1/\sqrt{r}$ gap also occurs with constant probability with respect to such a sequence. Unfortunately, we cannot benefit from this improvement, since the results of Haitner et al. [15] only guarantees indistinguishability for constant ρ, which makes it useful only for attacking constant-round protocols.

Let Z_i^{P} denote the backup value computed by party P in round i of a random execution of Π. The indistinguishability of $\widetilde{\mathsf{F}}$ yields that $\mathbf{E}\left[Z_i^{\mathsf{P}} \mid Y_{\leq i}\right] \approx Y_i^{\mathsf{P}}$. Similarly to the inefficient case, unless there is a simple $1/\sqrt{r}$-attack, it holds that

$$\text{Backup values approximate outcome:} \quad \Pr\left[\exists i \in [r]\colon \left|X_i - \mathbf{E}\left[Z_i^{\mathsf{P}} \mid Y_{\leq i}\right]\right| \geq 1/2\sqrt{r}\right] \leq 1/4 \tag{7}$$

So, to emulate the attack of Cleve and Impagliazzo [10], it suffices to prove that

$$\text{Independence:} \quad \mathbf{E}\left[Z_i^{\mathsf{P}} \mid Y_{\leq i}\right] \overset{\text{C}}{\approx}_{1/r} \mathbf{E}\left[Z_i^{\mathsf{P}} \mid Y_{\leq i+1}\right] \tag{8}$$

for every $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ and round i in which the other party sends the $(i+1)$ message. However, unlike Equation (3) in Section 1.2.1, Equation (8) might not be true. Rather, we show that if Equation (8) does not holds, then there exists a key-agreement protocol.

Proving that Y_{i+1} and Z_i^b are approximately independent given $Y_{\leq i}$, assuming inexistence of key agreement. We are now using a second result by Haitner et al. [15].[4]

Theorem 1.3 (Haitner et al. [15]'s dichotomy, informal)**.** *Let $\Delta = (\mathsf{A}, \mathsf{B})$ be an efficient single-bit output two-party protocol and assume i.o. key-agreement protocol does not exists. Then for any constant $\rho > 0$, there exists* PPT *algorithm (decorrelator) Dcr mapping transcripts of Δ into $[0,1] \times [0,1]$, such that the following holds. let (X, Y, T) be the parties outputs and transcript in a random execution of Δ, then,*[5]

$$(X, Y, T) \overset{\text{C}}{\approx}_{\rho} (U_{p^{\mathsf{A}}}, U_{p^{\mathsf{B}}}, T)_{(p^{\mathsf{A}}, p^{\mathsf{B}}) \leftarrow \mathsf{Dcr}(T)}.$$

Namely, assuming key-agreement do not exists, the distribution of the parties' output given the transcript, seems ρ close to the product distribution defined by Dcr. We assume for simplicity that the guaranteed forecaster is deterministic, and also assume that the theorem holds for *many-bit* output, and not merely for single bit, protocols (we get rid of this assumption in the actual proof).

We define another variant $\widehat{\pi}$ of Π that internally uses the forecaster $\widetilde{\mathsf{F}}$. We prove that assuming the existence of a decorrelator for $\widehat{\Pi}$, it holds that X_{i+1} and Z_i^{P} are approximately independent given $Y_{\leq i}$, and Equation (8) follows. For concreteness, we focus on party $\mathsf{P} = \mathsf{B}$.

Fix i such that A sends the $(i+1)$ message in Π. Let $\widehat{\pi} = (\widehat{\mathsf{A}}, \widehat{\mathsf{B}})$ be the protocol in which the parties interact just as in Π for the first i rounds. Then $\widehat{\mathsf{B}}$ outputs the i^{th} backup value of B, and $\widehat{\mathsf{A}}$ internally computes t_{i+1}, and outputs $y_{i+1} = \widetilde{\mathsf{F}}(i+1, t_{i+1})$. Assume key-agreement protocols do not exists, Theorem 1.3 yields the existence an efficient decorelator Dcr for $\widehat{\pi}$ with respect to $\rho = 1/r$. By definition, it holds that

$$(Y_{i+1}, Z_i^{\mathsf{B}}, T_i) \overset{\text{C}}{\approx}_{1/r} (U_{p^{\widehat{\mathsf{A}}}}, U_{p^{\widehat{\mathsf{B}}}}, T_i)_{(p^{\widehat{\mathsf{A}}}, p^{\widehat{\mathsf{B}}}) \leftarrow \mathsf{Dcr}(T_i)}, \tag{9}$$

where now $p^{\widehat{\mathsf{A}}}$ describes a non-Boolean distribution, and $U_{p^{\widehat{\mathsf{A}}}}$ denotes an independent sample from this distribution. Hence, to prove that Y_{i+1} and Z_i^{B} are approximately independent given $Y_{\leq i}$, it suffices to prove that $U_{p^{\widehat{\mathsf{A}}}}$ and $U_{p^{\widehat{\mathsf{B}}}}$ are approximately independent given $Y_{\leq i}$.

[4] Assuming the inexistence of key-agreement protocols, the following result implies the first result cited above. Yet, we chose to use both results to make the text more modular.

[5] Again, this is only guaranteed to hold for infinitely many lengths of the security parameter.

Since $\widetilde{\mathsf{F}}$ and Dcr both output the expected outcome of $Z_i^{\mathsf{B}}|T_i$ in a way that is indistinguishable from the real distribution of Z_i^{B} (given T_i), both algorithms output essentially the same value. Otherwise, at least one of the decorelators is far from the "real" value, and the other decorelator can be used to distinguish the real distribution from the emulated one. It follows that

$$(U_{p^{\widehat{\mathsf{A}}}}, U_{p^{\widehat{\mathsf{B}}}}, T_i)_{(p^{\widehat{\mathsf{A}}},p^{\widehat{\mathsf{B}}})\leftarrow\mathsf{Dcr}(T_i)} \overset{\mathrm{C}}{\approx}_{1/r} (U_{p^{\widehat{\mathsf{A}}}}, U_{Y_i^{\mathsf{B}}}, T_i)_{p^{\widehat{\mathsf{A}}}\leftarrow\mathsf{Dcr}(T_i)^{\widehat{\mathsf{A}}}} \tag{10}$$

Using a data-processing argument in combination with Equations (9) and (10), we deduce that

$$\left(Y_{i+1}, Z_i^{\mathsf{B}}, Y_{\leq i}\right) \overset{\mathrm{C}}{\approx}_{1/r} \left(U_{p^{\widehat{\mathsf{A}}}}, U_{p^{\widehat{\mathsf{B}}}}, Y_{\leq i}\right)_{(p^{\widehat{\mathsf{A}}},p^{\widehat{\mathsf{B}}})\leftarrow\mathsf{Dcr}(T_i)} \overset{\mathrm{C}}{\approx}_{1/r} \left(U_{p^{\widehat{\mathsf{A}}}}, U_{Y_i^{\mathsf{B}}}, Y_{\leq i}\right)_{p^{\widehat{\mathsf{A}}}\leftarrow\mathsf{Dcr}(T_i)^{\widehat{\mathsf{A}}}} \tag{11}$$

Finally, conditioned on $Y_{\leq i}$, the distribution of $(U_{p^{\widehat{\mathsf{A}}}}, U_{Y_i^{\mathsf{B}}})$ is a convex combination of product distributions of the form $(\cdot, U_{Y_i^{\widehat{\mathsf{B}}}})$, and thus it is a product distribution.

1.3 Related Work

We review some of the relevant work on fair coin-flipping protocols.

Necessary hardness assumptions. This line of work examines the minimal assumptions required to achieve an $o(1/\sqrt{r})$-bias two-party coin-flipping protocols, as done is this paper. Dachman-Soled et al. [11] have shown that any fully black-box construction of $O(1/r)$-bias two-party protocols based on one-way functions with r-bit input and output needs $\Omega(r/\log r)$ rounds. Dachman-Soled et al. [12] have shown that there is no fully black-box and function *oblivious* construction of $O(1/r)$-bias two-party protocols from one-way functions (a protocol is function oblivious if the outcome of the protocol is independent of the choice of the one-way function used in the protocol).

Lower bounds. Cleve [9] has proved that for every r-round two-party coin-flipping protocol there exists is an efficient adversary that can bias the output by $\Omega(1/r)$. Cleve and Impagliazzo [10] have proved that for every r-round two-party coin-flipping protocol there exists an inefficient fail-stop adversary that biases the output by $\Omega(1/\sqrt{r})$. They also showed that a similar attack exists also if the parties have access to an ideal commitment scheme. All above bounds extend to multi-party protocol (with no honest majority) via a simple reduction. Very recently, Beimel et al. [5] have shown that *any* r-round n-parties coin-flipping with $n^k > r$ for some $k \in \mathbb{N}$, can be biased by $1/(\sqrt{r} \cdot (\log r)^k)$. Ignoring logarithmic factors, this means that if the number of parties is $r^{\Omega(1)}$, the majority protocol of [3] is optimal.

Upper bounds. Blum [7] presented a two-party two-round coin-flipping protocol with bias $1/4$. Awerbuch et al. [3] presented an n-party r-round protocol with bias $O(n/\sqrt{r})$ (the two-party case appears also in Cleve [9]). Moran, Naor, and Segev [17] resolved the two-party case, presenting a two-party r-round coin-flipping protocol with bias $O(1/r)$. Haitner and Tsfadia [13] resolved the three-party case up to poly logarithmic factor, presenting a three-party coin-flipping protocol with bias $O(\mathrm{polylog}(r)/r)$. Buchbinder et al. [8] constructed an n-party r-round coin-flipping protocol with bias $\widetilde{O}(n^3 2^n / r^{\frac{1}{2}+\frac{1}{2^{n-1}-2}})$. In particular, their four-party coin-flipping protocol the bias is $\widetilde{O}(1/r^{2/3})$, and for $n = \log\log r$ their protocol has bias smaller than [3].

For the case where less than 2/3 of the parties are corrupt, Beimel et al. [4] have constructed an n-party r-round coin-flipping protocol with bias $2^{2^k}/r$, tolerating up to $t = (n+k)/2$ corrupt parties. Alon and Omri [1] constructed an n-party r-round coin-flipping protocol with bias $\widetilde{O}(2^{2^n}/r)$, tolerating up to t corrupted parties, for constant n and $t < 3n/4$.

Paper Organization

Basic definitions and notation used through the paper, are given in Section 2. The formal statement and proof of the main theorem are given in Section 3.

2 Preliminaries

2.1 Notation

We use calligraphic letters to denote sets, uppercase for random variables and functions, lowercase for values, and boldface for vectors. All logarithms considered here are in base two. For $a \in \mathbb{R}$ and $b \geq 0$, let $a \pm b$ stand for the interval $[a-b, a+b]$. For $n \in \mathbb{N}$, let $[n] := \{1, \ldots, n\}$ and $(n) := \{0, \ldots, n\}$. For $x, \delta \in [0,1]$ let $\mathsf{rnd}_\delta(x) = k\delta$, for $k \in \mathbb{Z}$ being the largest number with $k\delta \leq x$. Let poly denote the set of all polynomials, let PPT stand for probabilistic polynomial time, let PPTM denote a PPT algorithm (Turing machine). A function $\nu \colon \mathbb{N} \to [0,1]$ is *negligible*, denoted $\nu(n) = \mathrm{neg}(n)$, if $\nu(n) < 1/p(n)$ for every $p \in \mathrm{poly}$ and large enough n.

Given a distribution D, we write $x \leftarrow D$ to indicate that x is selected according to D. Similarly, given a random variable X, we write $x \leftarrow X$ to indicate that x is selected according to X. Given a finite set $\mathcal{S}$, we let $s \leftarrow \mathcal{S}$ denote that s is selected according to the uniform distribution on $\mathcal{S}$. The support of D, denoted $\mathrm{Supp}(D)$, be defined as $\{u \in \mathcal{U} : D(u) > 0\}$. The *statistical distance* between two distributions P and Q over a finite set $\mathcal{U}$, denoted as $\mathrm{SD}(P,Q)$, is defined as $\max_{\mathcal{S} \subseteq \mathcal{U}} |P(\mathcal{S}) - Q(\mathcal{S})| = \frac{1}{2}\sum_{u \in \mathcal{U}} |P(u) - Q(u)|$. Distribution ensembles $X = \{X_\kappa\}_{\kappa \in \mathbb{N}}$ and $Y = \{Y_\kappa\}_{\kappa \in \mathbb{N}}$ are *δ-computationally indistinguishable in the set $\mathcal{I}$*, denoted by $X \overset{\mathrm{C}}{\approx}_{\mathcal{I},\delta} Y$, if for every PPTM D and sufficiently large $\kappa \in \mathcal{I}$: $|\Pr[\mathsf{D}(1^\kappa, X_\kappa) = 1] - \Pr[\mathsf{D}(1^\kappa, Y_\kappa) = 1]| \leq \delta$.

2.2 Protocols

Let $\pi = (\mathsf{A}, \mathsf{B})$ be a two-party protocol. Protocol π is PPT if both A and B ruining time is polynomial in their input length. We denote by $(\mathsf{A}(x), \mathsf{B}(y))(z)$ a random execution of π with private inputs x and y, and common input z, and sometimes abuse notation and refer to $(\mathsf{A}(x), \mathsf{B}(y))(z)$ as the parties' output in this execution.

We will focus on no-input two-party protocol single-bit PPT output protocol: the two PPT parties only input is the common security parameter, given in unary, and at the end of the protocol each party output a single bit. Throughout, we assume without loss of generality that the transcript contains 1^κ as the first message. Let $\pi = (\mathsf{A}, \mathsf{B})$ be such two-party protocol single-bit. For $\kappa \in \mathbb{N}$, let $O_\kappa^{\mathsf{A},\pi}$, $O_\kappa^{\mathsf{B},\pi}$, and T_κ^π denote the A and B outputs respectively, and the execution transcript, in a random execution of $\pi(1^\kappa)$.

2.2.1 Fair Coin Flipping

Since we care of a lower bound, we only give the game base definition of coin flipping protocols (see [14] for the stronger simulation based definition).

Definition 2.1 (Fair coin-flipping protocols)**.** *A* PPT *single-bit output two-party protocol* $\pi = (\mathsf{A}, \mathsf{B})$ *is a an* ε*-fair coin-flipping protocol, if the following holds.*

Output delivery: *The honest party always output a bit (even if the other party acts dishonestly, or aborts).*

Aggrement: *The parties always output the same bit in an honest execution.*

Unifromity: $\Pr\left[O_\kappa^{\mathsf{A}} = b\right] = 1/2$ *(and thus* $\Pr\left[O_\kappa^{\mathsf{B}} = b\right] = 1/2$*), for both* $b \in \{0,1\}$ *and all* $\kappa \in \mathbb{N}$*.*

Fairness: *For any* PPT A^* *and* $b \in \{0,1\}$*, for sufficiently large* κ *it holds that*

$\Pr\left[O_\kappa^{\mathsf{B},(\mathsf{A}^*,\mathsf{B})} = b\right] \leq 1/2 + \varepsilon$*, and the same holds for the output bit of* A*.*

The proof of our main result easily extends to non optimal uniformity condition. Say, if we only require that $\Pr\left[O_\kappa^{\mathsf{A}} = b\right] \geq 1/4$ for both $b \in \{0,1\}$.

2.2.2 Key Agreement

We focus on single bit output key-agreement protocols.

Definition 2.2 (Key-agreement protocols)**.** *A* PPT *single-bit output two-party protocol* $\pi = (\mathsf{A}, \mathsf{B})$ *is* io key-agreement*, if there exist an infinite* $\mathcal{I} \subseteq \mathbb{N}$*, such that the following hold for* κ*'s in* $\mathcal{I}$*:*

Agreement. $\Pr\left[X_\kappa^\pi = Y_\kappa^\pi\right] \geq 1 - \mathrm{neg}(\kappa)$.

Secrecy. *For every* PPT Eve *it holds that* $\Pr\left[\mathsf{Eve}(T_\kappa^\pi) = X_\kappa^\pi\right] \leq 1/2 + \mathrm{neg}(\kappa)$.

2.3 Martingales

Definition 2.3 (martingales)**.** *Let* $X_0, \ldots, X_r$ *be a sequence of random variables. We say that the sequence is a martingale sequence if* $\mathbf{E}\left[X_{i+1} \mid X_{\leq i} = x_{\leq i}\right] = x_i$ *for every* $i \in [r-1]$*.*

In plain terms, a sequence is a strong martingale if the expectation of the next point conditioned on the entire history is exactly the last observed point.

Theorem 2.4. *Let* $X_0, \ldots, X_r$ *be a martingale sequence such that* $X_i \in [0,1]$*, for every* $i \in [r]$*. If* $X_0 = 1/2$ *and* $\Pr\left[X_r \in \{0,1\}\right] = 1$*, then* $\Pr\left[\exists i \in [r] \text{ s.t. } |X_i - X_{i-1}| \geq \frac{1}{4\sqrt{r}}\right] \geq \frac{1}{20}$.

3 Fair Coin-Flipping to Key Agreement

In this section we prove the main result of this work, stating that the existence of constant-round coin-flipping protocols, improving over the $1/\sqrt{r}$-bias majority protocol of [2], implies the existence of infinitely-often key-agreement. Formally, we prove the following theorem.

Theorem 3.1. *The following holds for any (constant) $r \in \mathbb{N}$: if there exists an r-round, $\frac{1}{25600\sqrt{r}}$-fair two-party coin-flipping protocol, see Definition 2.1, then there exists an infinitely-often key-agreement protocol.* [6]

The proof of Theorem 3.1 is formally given below. However, we first recall the high level description drawn in the introduction. We begin by using a good forecaster for the coin-flipping protocol π (which must exist, according to the existence of forecasters theorem of Haitner et al. [15]), for defining an efficiently computable game-value sequence for π: a sequence of efficiently computable random variables containing the expected outcome of the protocol given the forecaster's outputs. We then identify several properties of these values. The first condition is that the backup values (defenses for the case a premature abort) should be similar to the game-value sequence. Otherwise, an efficient attacker can use the forecaster to bias the output of the other party (this attack is applicable regardless of the existence of infinitely-often key-agreement). The second property is that since the game value sequence is a martingale, there must be a large jump ($\Omega(1/\sqrt{r})$) in the sequence value in some round. Hence by the first property, in such a round there must be a large gap between the game-value that the active party can compute, and the previous backup value of the other party. One might wish to exploit this gap by aborting whenever this gap is in its favor. Proving the success of the attack, however, requires a third property — the event that a gap is identified is (almost) *independent* of the backup value of the honest party. Indeed, if π does not imply infinitely-often key-agreement, then this third property follows by the dichotomy theorem of Haitner et al. [15]. Hence, we have shown that if io-key-agreement does not exist, protocol π is not $\Theta(1/\sqrt{r})$ fair, deriving a contradiction.

Moving to the formal proof, fix an r-round, two-party coin-flipping protocol $\pi = (\mathsf{A}, \mathsf{B})$ (we assume nothing about its fairness parameter for now). We associate the following random variables with a random honest execution of $\pi(1^\kappa)$. Let $M^\kappa = (M_1^\kappa, \ldots, M_r^\kappa)$ denote the message of the protocol and let O^κ denote the always common output of the parties. For $i \in \{0, \ldots, r\}$ and $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$, let $Z_i^{\mathsf{P},\kappa}$ be the "backup" value party P outputs, if the other party aborts after the i^{th} message was sent. In particular, $Z_r^{\mathsf{A},\kappa} = Z_r^{\mathsf{B},\kappa} = O^\kappa$ and $\Pr\left[Z_0^{\mathsf{P},\kappa} = 1\right] = 1/2$.

Forecaster for π. We are using a *forecaster* for π guaranteed by the following theorem (proof readily follows from Haitner et al. [15, Thm 3.8]).

Theorem 3.2 (Haitner et al. [15], existence of forecasters)**.** *Let Δ be a no-input, single-bit output two-party protocol. Then for any constant $\rho > 0$ there exists a* PPT *algorithm F (forecaster) mapping transcripts of Δ into (the binary description of) pairs in $[0,1] \times [0,1]$ and an infinite set $\mathcal{I} \in \mathbb{N}$, such that the following holds: let $O^{\mathsf{A},\kappa}$, $O^{\mathsf{B},\kappa}$ and T^κ denote the parties output and protocol transcript in a random execution of $\Delta(1^\kappa)$. Let $m(\kappa) \in \text{poly}$ be a bound on the number of coins used by F on transcripts in $\text{supp}(T^\kappa)$, and let S^κ be a uniform string of length $m(\kappa)$. Then*

- $(O^{\mathsf{A},\kappa}, T^\kappa, S^\kappa) \overset{\text{C}}{\approx}_{\rho,\mathcal{I}} (U_{p^{\mathsf{A}}}, T^\kappa, S^\kappa)_{(p^{\mathsf{A}},\cdot)=\mathsf{F}(T^\kappa;S^\kappa)}$, *and*
- $(O^{\mathsf{B},\kappa}, T^\kappa, S^\kappa) \overset{\text{C}}{\approx}_{\rho,\mathcal{I}} (U_{p^{\mathsf{B}}}, T^\kappa, S^\kappa)_{(\cdot,p^{\mathsf{B}})=\mathsf{F}(T^\kappa;S^\kappa)}$.

[6] Definition 2.1 requires perfect uniformity: the common output in an honest execution is an unbiased bit. The proof given below, however, easily extends to any non-trivial uniformity condition, e.g., the common output equals one with probability 3/4.

letting U_p be a Boolean random variable taking the value one with probability p.

Since we would like to have a forecaster for all (intermediate) backup value of π, we apply Theorem 3.2 with respect to protocol the following variant of π.

Protocol 3.3 ($\widetilde{\pi} = \left(\widetilde{\mathsf{A}}, \widetilde{\mathsf{B}}\right)$).

Common input: security parameter 1^κ.

Description:

1. $\widetilde{\mathsf{A}}$ *samples* $i \leftarrow [r]$ *and sends it to* $\widetilde{\mathsf{B}}$.
2. *The parties interact in the first i rounds of a random execution of $\pi(1^\kappa)$, with $\widetilde{\mathsf{A}}$ and $\widetilde{\mathsf{B}}$ taking the role of A and B receptively.*

   Let z_i^{A} and z_i^{B} be the i^{th} backup values of A and B as computed by the parties in the above execution.
3. $\widetilde{\mathsf{A}}$ *outputs* z_i^{A}, *and* $\widetilde{\mathsf{B}}$ *outputs* z_i^{B}.

Let $\gamma = 1/10^6 r^{3/2}$. Let $\mathcal{I} \subseteq \mathbb{N}$ and a PPT F be the infinite set and PPT forecaster resulting by applying Theorem 3.2 with respect to protocol $\widetilde{\pi}$ and $\rho = \gamma/2r$, and let S^κ denote a long enough uniform string to be used by F on transcripts of $\widetilde{\pi}(1^\kappa)$. We assume without loss of generality that the output length of F is *constant* (otherwise we chop each of its two outputs to its first $\lceil \log 1/\rho \rceil$ bits). An averaging argument yields that the following holds.

Claim 3.4. *Then for every $i \in [r]$:*

- $(Z_i^{\mathsf{A},\kappa}, M_{\leq i}^\kappa, S^\kappa) \overset{\text{C}}{\approx}_{\gamma,\mathcal{I}} (U_{p^{\mathsf{A}}}, M_{\leq i}^\kappa)_{(p^{\mathsf{A}},\cdot)=\mathsf{F}(M_{\leq i};S^\kappa)}$, *and*
- $(Z_i^{\mathsf{B},\kappa}, M_{\leq i}^\kappa, S^\kappa) \overset{\text{C}}{\approx}_{\gamma,\mathcal{I}} (U_{p^{\mathsf{B}}}, M_{\leq i}^\kappa)_{(\cdot,p^{\mathsf{B}})=\mathsf{F}(M_{\leq i};S^\kappa)}$

letting $\mathsf{F}(i, m_{\leq i}; r) = \mathsf{F}(m_{\leq i}; r)$

For $\kappa \in \mathbb{N}$, we define the random variables $Y_0^\kappa, \ldots, Y_r^\kappa$, by

$$Y_i^\kappa = (Y_i^{\mathsf{A},\kappa}, Y_i^{\mathsf{B},\kappa}) = \mathsf{F}(M_{\leq i}; S^\kappa). \tag{12}$$

Game values. To alleviate notation, we assume that the value of κ is determined by $|S^\kappa|$.

Definition 3.5 (game-value function). *For $\kappa \in \mathbb{N}$, $i \in [r]$, $y_{\leq i} \in \text{supp}(Y_{\leq i}^\kappa)$ and $s \in \text{Supp}(S^\kappa)$, let*

$$g(y_{\leq i}, s) = \mathbf{E}\left[O^\kappa \mid Y_{\leq i}^\kappa = y_{\leq i}, S^\kappa = s\right].$$

Namely,

Game values are efficiently approximateable. The following claim, proven in Section 3.1, tels us that the game values are efficiently approximateable.

Claim 3.6 (Game value sequence is efficiently approximateable)**.** *There exists* PPTM G *such that the following holds for every* $\kappa \in \mathbb{N}$ *and* $i \in [r]$*:*

$$\Pr\left[\mathsf{G}(Y^{\kappa}_{\leq i}, S^{\kappa}) \notin g(Y^{\kappa}_{\leq i}, S^{\kappa}) \pm \gamma\right] \leq \gamma/r.$$

Using a simple Markov argument, we deduce the following useful claim.

Claim 3.7. *Let* J *be an arbitrary random variable taking values in* $[r]$*. It holds that*

$$\mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J}, S^{\kappa}) - g(Y^{\kappa}_{\leq J}, S^{\kappa})\right] \in 2\gamma.$$

Forecasted backup values are close to game values. The following claim, proven in Section 3.2, states that condition on the output of the forecasters, the backup value are close to the game value.

Claim 3.8 (Forecasted backup values are close to game values)**.** *Assuming* π *is* $\frac{1}{6400\sqrt{r}}$*-fair, then for both* $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ *and large enough* $\kappa \in \mathcal{I}$*:*

$$\Pr\left[\exists i \in [r] \text{ s.t. } \left|g(Y^{\kappa}_{\leq i}, S^{\kappa}) - Y^{\mathsf{P},\kappa}_{i}\right| \geq 1/8\sqrt{r}\right] < 1/100.$$

Game values have large jump.

Claim 3.9 (Game values have large jump.)**.** *For every* $\kappa \in \mathbb{N}$*, it holds that* $\Pr\left[\exists i \in [r]\colon \left|g(Y^{\kappa}_{\leq i}, S^{\kappa}) - g(Y^{\kappa}_{\leq i-1}, S^{\kappa})\right| \geq 1/4\sqrt{r}\right] > 1/20.$

Proof. Consider the sequence of random variables $G^{\kappa}_0, \ldots, G^{\kappa}_r$ defined by $G^{\kappa}_i = g(Y^{\kappa}_{\leq i}, S^{\kappa})$. It is easy to see that this is a (strong) martingale sequence . Hence, since $G^{\kappa}_0 = 1/2$ and $G^{\kappa}_r \in \{0, 1\}$, the proof follows by Cleve and Impagliazzo [10] (see also [5]). □

Independence of attack decision. The following claim, proven in Section 3.3, will allow us to show if io key-agreement protocol does not exist, then one can exploit the above gap in the game value to bias the output of party B.

Claim 3.10 (Independence of attack decision)**.** *Let* C *be Boolean output* PPTM*. For* $\kappa \in \mathbb{N}$ *and* $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$*, let* $E^{\mathsf{P},\kappa}_1, \ldots, E^{\mathsf{P},\kappa}_r$ *be the sequence of random variables such that* $E^{\mathsf{P},\kappa}_i$ *is the indicator the event*

$$\mathsf{P} \text{ sends the } i^{\text{th}} \text{ message in } \pi(1^{\kappa}) \wedge \ \mathsf{C}(Y^{\kappa}_{\leq i}, S^{\kappa}) = 1.$$

Assume io key-agreement protocol does not exist, then for any $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ *and infinite subset* $\mathcal{I}' \subseteq \mathcal{I}$*, there exists an infinite set* $\mathcal{I}'' \subseteq \mathcal{I}'$ *such that for every* $\kappa \in \mathcal{I}''$*, and every* $i \in [r]$

$$\mathbf{E}\left[E^{\mathsf{P},\kappa}_i \cdot Z^{\overline{\mathsf{P}},\kappa}_{i-1} - E^{\mathsf{P},\kappa}_i \cdot Y^{\overline{\mathsf{P}},\kappa}_{i-1}\right] \in \pm 4\gamma,$$

where $\overline{\mathsf{P}}$ *denotes (the party in)* $\{\mathsf{A}, \mathsf{B}\} \setminus \{\mathsf{P}\}$*.*

Namely,

Putting it together.

Proof of Theorem 3.1. Let π be an $\varepsilon = \frac{1}{25600\sqrt{r}}$-fair coin flipping protocol.

Since π is $\frac{1}{6400\sqrt{r}} > \frac{1}{25600\sqrt{r}}$-fair, combining Claims 3.8 and 3.9 allow us to assume without loss of generality that there exists an infinite subset $\mathcal{I}' \subseteq \mathcal{I}$ such that

$$\Pr\left[\exists i \in [r]\colon \ \mathsf{A} \text{ sends } i^{\text{th}} \text{ message in } \pi(1^\kappa) \wedge g(Y^\kappa_{\leq i}, S^\kappa) - Y^{\mathsf{B},\kappa}_{i-1} \geq \frac{1}{8\sqrt{r}}\right] \geq \frac{1}{80} - \frac{1}{100} = \frac{1}{400} \quad (13)$$

Let C be the Boolean output PPTM such that, on input $(y_{\leq i} = ((y^{\mathsf{A}}_1, y^{\mathsf{B}}_1), \ldots, (y^{\mathsf{A}}_i, y^{\mathsf{B}}_i)), s)$, algorithm C outputs 1 if $\mathsf{G}(y_{\leq i}, s) - y^{\mathsf{B}}_{i-1} \geq 1/16\sqrt{r}$ and $\mathsf{G}(y_{\leq \ell}, s) - y^{\mathsf{B}}_{\ell-1} < 1/16\sqrt{r}$ for all $\ell < i$, and 0 otherwise. Furthermore, let $E^{\mathsf{A},\kappa}_i = E^\kappa_i$ be according to Claim 3.10 with respect to C. Let J^κ be the minimal i with $E^\kappa_i = 1$, setting it to $r+1$ if no such index exist . By Claim 3.6 and Equation (13), for every $\kappa \in \mathcal{I}'$:

$$\Pr\left[J^\kappa \neq r+1\right] > \frac{1}{400} - \gamma \geq \frac{1}{800} \quad (14)$$

and Claim 3.7 implies that for every such κ:

$$\mathbf{E}\left[g(Y^\kappa_{\leq J^\kappa}, S^\kappa) - \mathsf{G}(Y^\kappa_{\leq J^\kappa}, S^\kappa)\right] \in \pm 2\gamma. \quad (15)$$

Assume io key-agreement protocol does not exist, by Claim 3.10 we deduce that there exists an infinite set $\mathcal{I}''$ such that for every $\kappa \in \mathcal{I}''$, and every $i \in [r]$,

$$\mathbf{E}\left[E^\kappa_i \cdot Z^{\mathsf{B},\kappa}_{i-1} - E^\kappa_i \cdot Y^{\mathsf{B},\kappa}_{i-1}\right] \leq 4\gamma. \quad (16)$$

Hence,

$$\begin{aligned}\mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^\kappa-1} - Y^{\mathsf{B},\kappa}_{J^\kappa-1}\right] &= \sum_{i=1}^{r} \mathbf{E}\left[E^\kappa_i \cdot Z^{\mathsf{B},\kappa}_{i-1} - E^\kappa_i \cdot Y^{\mathsf{B},\kappa}_{i-1}\right] \\ &\in \pm r \cdot 4\gamma\end{aligned} \quad (17)$$

Consequently, using the fact that $\mathsf{G}(Y^\kappa_{\leq r}, S^\kappa) = Y^{\mathsf{B},\kappa}_r$, by Equations (14), (15) and (17), it follows that

$$\begin{aligned}&\mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^\kappa-1}\right] \\ &\quad= \mathbf{E}\left[g(Y^\kappa_{\leq J^\kappa}, S^\kappa)\right] - \mathbf{E}\left[\mathsf{G}(Y^\kappa_{\leq J^\kappa}, S^\kappa) - Y^{\mathsf{B},\kappa}_{J^\kappa-1}\right] + \mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^\kappa-1} - Y^{\mathsf{B},\kappa}_{J^\kappa-1}\right] - \mathbf{E}\left[g(Y^\kappa_{\leq J^\kappa}, S^\kappa) - \mathsf{G}(Y^\kappa_{\leq J^\kappa}, S^\kappa)\right] \\ &\quad\leq \frac{1}{2} - \mathbf{E}\left[\mathsf{G}(Y^\kappa_{\leq J^\kappa-1}, S^\kappa) - Y^{\mathsf{B},\kappa}_{J^\kappa-1} \mid J^\kappa \neq r+1\right] \cdot \Pr\left[J^\kappa \neq r+1\right] + 4r\gamma + 2\gamma \\ &\quad\leq \frac{1}{2} - \frac{1}{12800\sqrt{r}} + 8r\gamma \\ &\quad< \frac{1}{2} - \frac{1}{25600\sqrt{r}}.\end{aligned}$$

The last inequality follows from our choice of $\gamma = \frac{1}{10^6 r^{3/2}}$.

The above yields that the following PPT fail-stop attacker A^* taking the role of A in π, biasing the output of B towards zero by $1/(25600\sqrt{r})$ for all $\kappa \in \mathcal{I}''$, contradicting the assume fairness of π.

Algorithm 3.11 (A^*)**.**

Input: security parameter 1^κ.

Description:

1. *Samples* $s \leftarrow S^\kappa$ *and start a random execution of* $\mathsf{A}(1^\kappa)$.
2. *Upon receiving the* $(i-1)$ *message* m_{i-1}*, do*
   (a) *Forward* m_{i-1} *to* A*, and let* m_i *be the next message sent by* A.
   (b) *Compute* $y_i = (y_i^{\mathsf{A}}, y_i^{\mathsf{B}}) = \mathsf{F}(m_{\leq i}, s)$.
   (c) *Compute* $\widetilde{g}_i = \mathsf{G}(y_{\leq i}, s)$.
   (d) *If* $\widetilde{g}_i \geq y_{i-1}^{\mathsf{B}} + 1/16\sqrt{r}$*, abort (without sending further messages). Otherwise, send* m_i *to* B *and proceed to the next round.*

□

3.1 Game Values are Efficiently Approximateable

In this section we prove Claim 3.6,

Claim 3.12 (Claim 3.6, restated)**.** *There exists* PPTM G *such that the following holds for every* $\kappa \in \mathbb{N}$ *and* $i \in [r]$*:*

$$\Pr\left[\mathsf{G}(Y_{\leq i}^\kappa, S^\kappa) \notin g(Y_{\leq i}^\kappa, S^\kappa) \pm \gamma\right] \leq \gamma/r.$$

Intuitively, for security parameter κ randomness s and forecasted sequence $y_{\leq i}$, the algorithm samples $(2r)^{500r}$ transcripts of $\pi(1^\kappa)$ and counts how many times the protocol outputs one while the forecaster (with fixed randomness s) predicts the sequence $y_{\leq i}$ for those transcripts. Unless $y_{\leq i}$ is very uniquely, we have a good grasp of how close the output of the algorithm is to the "true" value.

Remark 3.13. *The exponential dependency in* r *can be reduced to polynomial using the techniques of Beimel et al. [5]. Unfortunately, we cannot benefit from this improvement, since the results of Haitner et al. [15] only guarantees indistinguishability for constant* ρ*, which makes it useful only for attacking constant-round protocols.*

Proof of Claim 3.12 . The approximation algorithm is defined as follows.

Algorithm 3.14 (G, approximating g)**.**

Parameters: $y_{\leq i} \in \mathrm{supp}(Y_{\leq i}^\kappa)$

Description:

1. *Set* $\left\{m^{\ell}_{\leq r}\right\}_{\ell=1\ldots(2r)^{500r}}$ *to be* $(2r)^{500r}$ *transcripts of* π*, obtained by running* $(2r)^{500r}$ *independent instances of protocol* $\pi(1^{\kappa})$*.*
2. *Set* $\left\{\mathsf{out}^{\ell}\right\}_{\ell=1\ldots(2r)^{500r}}$ *to be* $(2r)^{500r}$ *bits where* out^{ℓ} *is the output of* π *for transcript* $m^{\ell}_{\leq r}$*.*
3. *For every* $\ell \in [(2r)^{500r}]$ *and* $j \in [i]$*, compute* $y^{\ell}_{j} = \mathsf{F}(m^{\ell}_{\leq j}, s)$*.*
4. *Compute* $p = \left|\ell \in [(2r)^{500r}] \colon y^{\ell}_{\leq i} = y_{\leq i} \wedge \mathsf{out}^{\ell} = 1\right|$ *and* $q = \left|\ell \in [(2r)^{500r}] \colon y^{\ell}_{\leq i} = y_{\leq i}\right|$*.*
5. *if* $q \neq 0$*, set* $\widetilde{g} = p/q$*. Otherwise, set* $\widetilde{g} = 0$*.*
6. *Output* $\widetilde{g}$*.*

Next, we analyze the accuracy of G. It suffices to prove the claim for every fixed $s \in \mathrm{supp}(S^{\kappa})$, i.e.

$$\Pr_{m_{\leq i} \leftarrow M^{\kappa}_{\leq i}}\left[\left|\mathsf{G}(\mathsf{F}(m_{\leq j}, s))_{j \leq i}, s\right) - g((\mathsf{F}(m_{\leq j}, s))_{j \leq i}, s)\right| \geq \gamma\right] \leq \frac{\gamma}{r}, \tag{18}$$

where the probability is taken over $M^{\kappa}_{\leq i}$ and the random coins of G. Fix $y_{\leq i}$ such that $\Pr_{m_{\leq i} \leftarrow M^{\kappa}_{\leq i}}\left[(\mathsf{F}(m_{\leq j}, s))_{j \leq i} = y_{\leq i}\right] \geq (2r)^{-100r}$. Using standard approximation via sampling techniques, we deduce that

$$\begin{aligned}
\Pr\left[\left|g(y_{\leq i}, s) - \mathsf{G}(y_{\leq i}, s)\right| \geq 3 \cdot (2r)^{-100r}\right] &\leq 4 \cdot \exp\left(-2 \cdot (2r)^{500r} \cdot \left((2r)^{-100r}\right)^{4}\right) \\
&\leq 4 \cdot \exp\left(-2 \cdot (2r)^{100r}\right) \\
&\leq \frac{\gamma}{2r}.
\end{aligned}$$

Since $\Pr\left[\left|g(y_{\leq i}, s) - \mathsf{G}(y_{\leq i}, s)\right| \geq 3 \cdot (2r)^{-100r}\right] \geq \Pr\left[\left|g(y_{\leq i}, s) - \mathsf{G}(y_{\leq i}, s)\right| \geq \gamma\right]$ and the probability of sampling such $y_{\leq i}$ is at least $1 - (2r)^{-100r} \cdot \left|\mathrm{supp}(Y^{\kappa}_{\leq i})\right|$, it follows that

$$\begin{aligned}
&\Pr_{m_{\leq i} \leftarrow M^{\kappa}_{\leq i}}\left[\left|\mathsf{G}(\mathsf{F}(m_{\leq j}, s))_{j \leq i}, s\right) - g((\mathsf{F}(m_{\leq j}, s))_{j \leq i}, s)\right| \geq \gamma\right] \\
&\quad \leq \frac{\gamma}{2r} + (2r)^{-100r} \cdot \left|\mathrm{supp}(Y^{\kappa}_{\leq i})\right|.
\end{aligned}$$

To conclude, we recall that $(2r)^{-100r} \cdot \left|\mathrm{supp}(Y^{\kappa}_{\leq i})\right| \leq (2r)^{-100r} \cdot \left|\mathrm{supp}(Y^{\kappa}_{\leq r})\right| = (2r)^{-100r}\left(\frac{1}{\rho}\right)^{r} = (2r)^{-100r}\left(\frac{2r}{\gamma}\right)^{r} \leq \frac{\gamma}{2r}$, since $\gamma = \frac{1}{10^{6} r^{3/2}}$.

□

3.2 Forecasted Backup Values are Close to Game Values

In this section we prove Claim 3.8,

Claim 3.15 (Claim 3.8, restated)**.** *Assuming* π *is* $\frac{1}{6400\sqrt{r}}$*-fair, then for both* $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ *and large enough* $\kappa \in \mathcal{I}$*:*

$$\Pr\left[\exists i \in [r] \ \textit{s.t.} \ \left|g(Y^{\kappa}_{\leq i}, S^{\kappa}) - Y^{\mathsf{P},\kappa}_{i}\right| \geq 1/8\sqrt{r}\right] < 1/100.$$

Proof of Claim 3.15. Assume the claim does not holds for $\mathsf{P} = \mathsf{B}$ and infinitely many security parameters $\mathcal{I}$ (the case $\mathsf{P} = \mathsf{A}$ is proven analogously). That is, for all $\kappa \in \mathcal{I}$ without loss of generality it holds that

$$\Pr\left[\exists i \in [r] \text{ s.t. } g(Y^{\kappa}_{\leq i}, S^{\kappa}) - Y^{\mathsf{B},\kappa}_{i} \geq \frac{1}{8\sqrt{r}}\right] \geq \frac{1}{200}. \tag{19}$$

Consider the following PPT fail-stop attacker A^* taking the role of A in π, to bias the output of B towards zeros.

Algorithm 3.16 (A^*)**.**

Input: security parameter 1^{κ}.

Description:

1. *Samples* $s \leftarrow S^{\kappa}$ *and start a random execution of* $\mathsf{A}(1^{\kappa})$.
2. *For* $i = 1 \ldots r$*:*

   After sending (or receiving) the prescribed message m_i*:*

   (a) *Compute* $y_i = \mathsf{F}(m_{\leq i}, s)$ *and* $\mu_i = \mathsf{G}(y_{\leq i}, s) - y_i$.

   (b) *If* $\mu_i \geq \frac{1}{8\sqrt{r}} - \gamma$*, abort (without sending further messages). Otherwise, proceed to the next round.*

In the following fix $\kappa \in \mathcal{I}$ such that Equation (19) holds. It remains to show that Algorithm 3.16 achieves a bias of at least $\frac{1}{6400\sqrt{r}}$ towards zero.

First we define the following random variable. Let J^{κ} denote the index where the adversary aborted, i.e. the smallest j such that $\mathsf{G}(Y^{\kappa}_{\leq j}, S^{\kappa}) - Y^{\mathsf{B},\kappa}_{j} \geq \frac{1}{8\sqrt{r}} - \gamma$, or $J^{\kappa} = r$ if no abort occurred. The following expectations are taken over $Y^{\kappa}_{\leq i}, S^{\kappa}$ and the random coins of G. We bound $\mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^{\kappa}}\right]$, i.e. the expected output of the honest party.

$$\begin{aligned}
\mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^{\kappa}}\right] &= \mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^{\kappa}}\right] + \mathbf{E}\left[g(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa})\right] - \mathbf{E}\left[g(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa})\right] + \mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right] - \mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right] \\
&= \mathbf{E}\left[g(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa})\right] - \mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right] + \mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - g(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa})\right] + \mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^{\kappa}} - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right] \\
&= \frac{1}{2} - \mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right] + \mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - g(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa})\right] + \mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^{\kappa}} - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right].
\end{aligned} \tag{20}$$

he last equation follows from the fact that $\mathbf{E}\left[g(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa})\right] = \mathbf{E}\left[\mathsf{out}\right]$ and thus $\mathbf{E}\left[g(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa})\right] = \frac{1}{2}$. Next, we bound each of the terms above separately. Observe that

$$\begin{aligned}
\Pr\left[J^{\kappa} \neq r\right] &\geq \Pr\left[\left(\forall i \in [r]\colon \left|\mathsf{G}(Y^{\kappa}_{\leq i}, S^{\kappa}) - g(Y^{\kappa}_{\leq i}, S^{\kappa})\right| \leq \gamma\right) \wedge \left(\exists j \in [r]\colon G_j - Y^{\mathsf{B},\kappa}_{j} \geq \frac{1}{8\sqrt{r}}\right)\right] \\
&\geq \Pr\left[\exists j \in [r]\colon G_j - Y^{\kappa}_{j} \geq \frac{1}{8\sqrt{r}}\right] - \Pr\left[\exists i \in [r]\colon \left|\mathsf{G}(Y^{\kappa}_{\leq i}, S^{\kappa}) - g(Y^{\kappa}_{\leq i}, S^{\kappa})\right| > \gamma\right] \\
&\geq \frac{1}{200} - \gamma \geq \frac{1}{400}.
\end{aligned}$$

Using the fact that $\mathsf{G}(Y^{\kappa}_{\leq r}, S^{\kappa}) = Y^{\mathsf{B},\kappa}_{r}$, it follows that

$$\begin{aligned}\mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right] &= \Pr\left[J^{\kappa} \neq r\right] \cdot \mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right] \\ &\geq \frac{1}{400} \cdot \left(\frac{1}{8\sqrt{r}} - \gamma\right). \end{aligned} \tag{21}$$

By Claim 3.7,

$$\mathbf{E}\left[\mathsf{G}(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa}) - g(Y^{\kappa}_{\leq J^{\kappa}}, S^{\kappa})\right] \leq 2\gamma. \tag{22}$$

Finally, since $Y^{\kappa}_{\leq i}$ uniquely determines $J = i$, by the forecaster's indistinguishability ,

$$\mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^{\kappa}} - Y^{\mathsf{B},\kappa}_{J^{\kappa}}\right] \leq \gamma. \tag{23}$$

By Equations (20) to (23), we deduce that $\mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^{\kappa}}\right] \leq \frac{1}{2} - \frac{1}{3200\sqrt{r}} + 4\gamma$. Since $\gamma = \frac{1}{10^6 r^{3/2}}$, we deduce that $\mathbf{E}\left[Z^{\mathsf{B},\kappa}_{J^{\kappa}}\right] < \frac{1}{2} - \frac{1}{6400\sqrt{r}}$.

□

3.3 Independence of Attack Decision

In this section we prove Claim 3.10, restated blow.

Claim 3.17 (Claim 3.10, restated)**.** *Let* C *be Boolean output* PPTM*. For* $\kappa \in \mathbb{N}$ *and* $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$*, let* $E^{\mathsf{P},\kappa}_1, \ldots, E^{\mathsf{P},\kappa}_r$ *be the sequence of random variables such that* $E^{\mathsf{P},\kappa}_i$ *is the indicator the event*

$$\mathsf{P} \text{ sends the } i^{\text{th}} \text{ message in } \pi(1^{\kappa}) \wedge\ \mathsf{C}(Y^{\kappa}_{\leq i}, S^{\kappa}) = 1.$$

Assume io key-agreement protocol does not exist, then for any $\mathsf{P} \in \{\mathsf{A}, \mathsf{B}\}$ *and infinite subset* $\mathcal{I}' \subseteq \mathcal{I}$*, there exists an infinite set* $\mathcal{I}'' \subseteq \mathcal{I}'$ *such that for every* $\kappa \in \mathcal{I}''$*, and every* $i \in [r]$

$$\mathbf{E}\left[E^{\mathsf{P},\kappa}_i \cdot Z^{\overline{\mathsf{P}},\kappa}_{i-1} - E^{\mathsf{P},\kappa}_i \cdot Y^{\overline{\mathsf{P}},\kappa}_{i-1}\right] \in \pm 4\gamma,$$

where $\overline{\mathsf{P}}$ *denotes (the party in)* $\{\mathsf{A}, \mathsf{B}\} \setminus \{\mathsf{P}\}$*.*

We prove for $\mathsf{P} = \mathsf{A}$. Consider the following variant of π.

Protocol 3.18 ($\widehat{\Pi} = \left(\widehat{\mathsf{A}}, \widehat{\mathsf{B}}\right)$)**.**

Common input: security parameter 1^{κ}*.*

Description:

1. *Party* $\widehat{\mathsf{A}}$ *samples* $i \leftarrow [r]$ *and* $s \leftarrow S^{\kappa}$*, and sends them to* $\widehat{\mathsf{B}}$*.*
2. *The parties interact in the first* $i - 1$ *rounds of a random execution of* $\pi(1^{\kappa})$*, with* $\widehat{\mathsf{A}}$ *and* $\widehat{\mathsf{B}}$ *taking the role of* A *and* B *respectively.*

   Let $m_1, \ldots, m_{i-1}$ *be the messages, and let* z^{B}_{i-1} *be the* $(i-1)$ *backup output of* B *in the above execution.*

3. $\widehat{\mathsf{A}}$ *sets the value of* e_i^{A} *as follows:*

   If A *sends the* $i-1$ *message above, then it sets* $e_i^{\mathsf{A}} = 0$.

   Otherwise, it

   (a) *Continues the above execution of* π *to compute its next message* m_i.

   (b) *Computes* $y_i = (y_i^{\mathsf{A}}, y_i^{\mathsf{B}}) = \mathsf{F}(m_{\leq i}, s)$.

   (c) *Let* $e_i^{\mathsf{A}} = \mathsf{C}(y_{\leq i}, s)$.

4. $\widehat{\mathsf{A}}$ *outputs* e_i^{A} *and* B *outputs* z_{i-1}^{B}.

We use the following dichotomy result of Haitner et al. [15].

Theorem 3.19 (Haitner et al. [15], Thm. 3.18, dichotomy of two-party protocols)**.** *Let* Δ *be an efficient single-bit output two-party protocol. Assume io key-agreement protocol does not exits, then for any constant* $\rho > 0$ *and infinite subset* $\mathcal{I} \subseteq \mathbb{N}$*, there exists a* PPT *algorithm* Dcr *(decorelator) mapping transcripts of* Δ *into (the binary description of) pairs in* $[0,1] \times [0,1]$ *and an infinite set* $\mathcal{I}' \in \mathbb{N}$*, such that the following holds: let* $O^{\mathsf{A},\kappa}$*,* $O^{\mathsf{B},\kappa}$ *and* T^κ *denote the parties output and protocol transcript in a random execution of* $\Delta(1^\kappa)$*. Let* $m(\kappa) \in \text{poly}$ *be a bound on the number of coins used by* F *on transcripts in* $\text{supp}(T^\kappa)$*, and let* S^κ *be a uniform string of length* $m(\kappa)$*. Then*

$$(O^{\mathsf{A},\kappa}, O^{\mathsf{B},\kappa}, T^\kappa, S^\kappa) \overset{\text{C}}{\approx}_{\rho,\mathcal{I}'} (U_{p^{\mathsf{A}}}, U_{p^{\mathsf{A}}}, T^\kappa, S^\kappa)_{(p^{\mathsf{A}},p^{\mathsf{B}})=\mathsf{Dcr}(T^\kappa;S^\kappa)}$$

letting U_p *be a Boolean random variable taking the value one with probability* p*.*

Assume io key-agreement does not exits. Let $\mathcal{I}'' \subseteq \mathcal{I}'$ and a PPT Dcr be the infinite set and PPT decorelator resulting by applying Theorem 3.19 with respect to protocol $\widehat{\Pi}$ and $\rho = \gamma/r$. Let $\widehat{S}^\kappa$ denote a long enough uniform string to be used by Dcr on transcripts of $\widehat{\Pi}(1^\kappa)$. An averaging argument yields that the following holds for every $i \in [r]$:

$$(E_i^{\mathsf{A},\kappa}, Z_{i-1}^{\mathsf{B},\kappa}, M_{\leq i-1}^\kappa, S^\kappa, \widehat{S}^\kappa) \overset{\text{C}}{\approx}_{\gamma,\mathcal{I}''} (U_{p^{\mathsf{A}}}, U_{p^{\mathsf{B}}}, M_{\leq i-1}^\kappa, S^\kappa, \widehat{S}^\kappa)_{(p^{\mathsf{A}},p^{\mathsf{B}})=\mathsf{Dcr}(M_{\leq i},S^\kappa;\widehat{S}^\kappa)} \tag{24}$$

letting $\mathsf{Dcr}(m_{\leq i}, s; \widehat{s}) = \mathsf{Dcr}(i, s, m_{\leq i}; \widehat{s})$. For $i \in [r]$, let $W_i^\kappa = (W_i^{\mathsf{A},\kappa}, W_i^{\mathsf{B},\kappa}) = \mathsf{Dcr}(M_{\leq i}, S^\kappa; \widehat{S}^\kappa)$. The theorem follows immediately from the three claims below.

Claim 3.20. *For* $\kappa \in \mathcal{I}''$*, for every* $i \in [r]$*, it holds that* $\mathbf{E}\left[E_i^{\mathsf{A},\kappa} \cdot Z_{i-1}^{\mathsf{B},\kappa} - W_{i-1}^{\mathsf{A},\kappa} \cdot W_{i-1}^{\mathsf{B},\kappa}\right] \in \pm\gamma$.

Proof. Observe that $\mathbf{E}\left[W_{i-1}^{\mathsf{A},\kappa} W_{i-1}^{\mathsf{B},\kappa}\right] = \mathbf{E}\left[U_{W_{i-1}^{\mathsf{A},\kappa}} U_{W_{i-1}^{\mathsf{B},\kappa}}\right]$. Consider the following the following algorithm D: for input $(z^{\mathsf{A}}, z^{\mathsf{B}}, (m_{\leq i-1}, s))$, output $z^{\mathsf{A}} \cdot z^{\mathsf{B}}$. By noting that D outputs 1 with probability $\mathbf{E}\left[U_{W_{i-1}^{\mathsf{A},\kappa}} U_{W_{i-1}^{\mathsf{B},\kappa}}\right]$ and $\mathbf{E}\left[E_i^{\mathsf{A},\kappa} \cdot Z_{i-1}^{\mathsf{B},\kappa}\right]$ for input $(U_{W_{i-1}^{\mathsf{A},\kappa}}, U_{W_{i-1}^{\mathsf{B},\kappa}}, (M_{\leq i-1}^\kappa, S^\kappa))$ and $(E_i^{\mathsf{A},\kappa}, Z_{i-1}^{\mathsf{B},\kappa}, (M_{\leq i-1}^\kappa, S^\kappa))$, respectively, our claim follows by applying Equation (24). □

Claim 3.21. *For* $\kappa \in \mathcal{I}''$*, for every* $i \in [r]$*, it holds that* $\mathbf{E}\left[W_{i-1}^{\mathsf{A},\kappa} \cdot W_{i-1}^{\mathsf{B},\kappa} - W_{i-1}^{\mathsf{A},\kappa} \cdot Y_{i-1}^{\mathsf{B},\kappa}\right] \in \pm 2\gamma$.

Proof. Since $\left|W_{i-1}^{\mathsf{A},\kappa}\right| \leq 1$, it suffices to prove $\mathbf{E}\left[\left|W_{i-1}^{\mathsf{B},\kappa} - Y_{i-1}^{\mathsf{B},\kappa}\right|\right] \leq 2\gamma$. We show that if $\mathbf{E}\left[\left|W_{i-1}^{\mathsf{B},\kappa} - Y_{i-1}^{\mathsf{B},\kappa}\right|\right] > 2\gamma$, then there exists a distinguisher with advantage greater than γ for either the real outputs of $\widehat{\Pi}$ and the emulated outputs of Dcr, or, the real outputs of $\widetilde{\pi}$ and the emulated outputs of F, in contradiction with the assumed properties of Dcr and F. Define the following algorithm D: for security parameter 1^κ and input $(z^{\mathsf{A}}, z^{\mathsf{B}}, (m_{\leq i-1}, s))$, sample $\widehat{s} \leftarrow \widehat{S}^\kappa$, and compute $(\cdot, y^{\mathsf{B}}) = \mathsf{F}(m_{\leq i-1}; s)$ and $(\cdot, w^{\mathsf{B}}) = \mathsf{Dcr}(m_{\leq i-1}, s; \widehat{s})$. The algorithm outputs z^{B} if $w^{\mathsf{B}} \geq y^{\mathsf{B}}$, and $1 - z^{\mathsf{B}}$ otherwise. We compute the difference in probability that D outputs 1 given a sample from Dcr and a sample from F.

$$
\begin{aligned}
&\Pr\left[\mathsf{D}(U_{W_{i-1}^{\mathsf{A},\kappa}}, U_{W_{i-1}^{\mathsf{B},\kappa}}, (M_{\leq i-1}^\kappa, S^\kappa)) = 1\right] - \Pr\left[\mathsf{D}(U_{Y_{i-1}^{\mathsf{A},\kappa}}, U_{Y_{i-1}^{\mathsf{B},\kappa}}, (M_{\leq i-1}^\kappa, S^\kappa)) = 1\right] \\
&\quad = \mathbf{E}\left[U_{W_{i-1}^{\mathsf{B},\kappa}} \mid W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] \cdot \Pr\left[W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] + \mathbf{E}\left[1 - U_{W_{i-1}^{\mathsf{B},\kappa}} \mid W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \cdot \Pr\left[W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \\
&\qquad - \mathbf{E}\left[U_{Y_{i-1}^{\mathsf{B},\kappa}} \mid W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] \cdot \Pr\left[W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] - \mathbf{E}\left[1 - U_{Y_{i-1}^{\mathsf{B},\kappa}} \mid W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \cdot \Pr\left[W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \\
&\quad = \mathbf{E}\left[W_{i-1}^{\mathsf{B},\kappa} \mid W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] \cdot \Pr\left[W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] - \mathbf{E}\left[W_{i-1}^{\mathsf{B},\kappa} \mid W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \Pr\left[W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \\
&\qquad - \mathbf{E}\left[Y_{i-1}^{\mathsf{B},\kappa} \mid W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] \cdot \Pr\left[W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] + \mathbf{E}\left[Y_{i-1}^{\mathsf{B},\kappa} \mid W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \cdot \Pr\left[W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \\
&\quad = \mathbf{E}\left[W_{i-1}^{\mathsf{B},\kappa} - Y_{i-1}^{\mathsf{B},\kappa} \mid W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] \cdot \Pr\left[W_{i-1}^{\mathsf{B},\kappa} \geq Y_{i-1}^{\mathsf{B},\kappa}\right] \\
&\qquad + \mathbf{E}\left[-W_{i-1}^{\mathsf{B},\kappa} + Y_{i-1}^{\mathsf{B},\kappa} \mid W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \Pr\left[W_{i-1}^{\mathsf{B},\kappa} < Y_{i-1}^{\mathsf{B},\kappa}\right] \\
&\quad = \mathbf{E}\left[\left|W_{i-1}^{\mathsf{B},\kappa} - Y_{i-1}^{\mathsf{B},\kappa}\right|\right] \\
&\quad > 2\gamma
\end{aligned}
$$

A simple averaging argument yields that D is a distinguisher with advantage greater than γ for either $(U_{Y_{i-1}^{\mathsf{A},\kappa}}, U_{Y_{i-1}^{\mathsf{B},\kappa}}, (M_{\leq i-1}^\kappa, S^\kappa))$ and $(Z_{i-1}^{\mathsf{A},\kappa}, Z_{i-1}^{\mathsf{B},\kappa}, (M_{\leq i-1}^\kappa, S^\kappa))$, or, $(U_{W_{i-1}^{\mathsf{A},\kappa}}, U_{W_{i-1}^{\mathsf{B},\kappa}}, (M_{\leq i-1}^\kappa, S^\kappa))$ and $(E_i^{\mathsf{A},\kappa}, Z_{i-1}^{\mathsf{B},\kappa}, (M_{\leq i-1}^\kappa, S^\kappa))$. □

Claim 3.22. *For $\kappa \in \mathcal{I}''$, for every $i \in [r]$, it holds that $\mathbf{E}\left[W_{i-1}^{\mathsf{A},\kappa} \cdot Y_{i-1}^{\mathsf{B},\kappa} - E_i^{\mathsf{A},\kappa} \cdot Y_{i-1}^{\mathsf{B},\kappa}\right] \in \pm\gamma$.*

Proof. Observe that $\mathbf{E}\left[W_{i-1}^{\mathsf{A},\kappa} Y_{i-1}^{\mathsf{B},\kappa} - E_i^{\mathsf{A},\kappa} \cdot Y_{i-1}^{\mathsf{B},\kappa}\right] = \mathbf{E}\left[U_{W_{i-1}^{\mathsf{A},\kappa}} U_{Y_{i-1}^{\mathsf{B},\kappa}} - E_i^{\mathsf{A},\kappa} \cdot U_{Y_{i-1}^{\mathsf{B},\kappa}}\right]$. Consider the following the following algorithm D: for security parameter 1^κ and input $(z^{\mathsf{A}}, z^{\mathsf{B}}, (m_{\leq i-1}, s))$, compute $(\cdot, y^{\mathsf{B}}) = \mathsf{F}(m_{\leq i-1}; s)$ and sample $u \leftarrow U_{y^{\mathsf{B}}}$. Output $z^{\mathsf{A}} \cdot u$. By noting that D outputs 1 with probability $\mathbf{E}\left[U_{W_{i-1}^{\mathsf{A},\kappa}} U_{Y_{i-1}^{\mathsf{B},\kappa}}\right]$ and $\mathbf{E}\left[E_i^{\mathsf{A},\kappa} \cdot U_{Y_{i-1}^{\mathsf{B},\kappa}}\right]$ for input $(U_{W_{i-1}^{\mathsf{A},\kappa}}, U_{W_{i-1}^{\mathsf{B},\kappa}}, (M_{\leq i-1}^\kappa, S^\kappa))$ and $(E_i^{\mathsf{A},\kappa}, Z_{i-1}^{\mathsf{B},\kappa}, (M_{\leq i-1}^\kappa, S^\kappa))$, respectively, we apply Equation (24), and we deduce that $\mathbf{E}\left[U_{W_{i-1}^{\mathsf{A},\kappa}} U_{Y_{i-1}^{\mathsf{B},\kappa}} - E_i^{\mathsf{A},\kappa} \cdot U_{Y_{i-1}^{\mathsf{B},\kappa}}\right] \in \pm\gamma$. □

References

[1] B. Alon and E. Omri. Almost-optimally fair multiparty coin-tossing with nearly three-quarters malicious. In *Proceedings of the 14th Theory of Cryptography Conference, TCC 2016-B, part I*, pages 307–335, 2016.

[2] B. Averbuch, M. Blum, B. Chor, S. Goldwasser, and S. Micali. How to implement Bracha's $O(\log n)$ Byzantine agreement algorithm, 1985. Unpublished manuscript.

[3] B. Awerbuch, M. Blum, B. Chor, S. Goldwasser, and S. Micali. How to implement Bracha's $O(\log n)$ byzantine agreement algorithm. Unpublished manuscript, 1985.

[4] A. Beimel, E. Omri, and I. Orlov. Protocols for multiparty coin toss with a dishonest majority. *Journal of Cryptology*, 28(3):551–600, 2015.

[5] A. Beimel, I. Haitner, N. Makriyannis, and E. Omri. Tighter bounds on multi-party coin flipping, via augmented weak martingales and differentially private sampling. Technical Report TR17-168, Electronic Colloquium on Computational Complexity, 2017.

[6] I. Berman, I. Haitner, and A. Tentes. Coin flipping of any constant bias implies one-way functions. *Journal of the ACM*, 65(3):14, 2018.

[7] M. Blum. How to exchange (secret) keys. *ACM Transactions on Computer Systems*, 1983.

[8] N. Buchbinder, I. Haitner, N. Levi, and E. Tsfadia. Fair coin flipping: Tighter analysis and the many-party case. In *Proceedings of the 28th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 2580–2600, 2017.

[9] R. Cleve. Limits on the security of coin flips when half the processors are faulty. In *Proceedings of the 18th Annual ACM Symposium on Theory of Computing (STOC)*, pages 364–369, 1986.

[10] R. Cleve and R. Impagliazzo. Martingales, collective coin flipping and discrete control processes (extended abstract). http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.51.1797, 1993.

[11] D. Dachman-Soled, Y. Lindell, M. Mahmoody, and T. Malkin. On the black-box complexity of optimally-fair coin tossing. In *Proceedings of the 8th Theory of Cryptography Conference, TCC 2011*, volume 6597, pages 450–467, 2011.

[12] D. Dachman-Soled, M. Mahmoody, and T. Malkin. Can optimally-fair coin tossing be based on one-way functions? In Y. Lindell, editor, *Theory of Cryptography - 11th Theory of Cryptography Conference, TCC 2014*, volume 8349 of *Lecture Notes in Computer Science*, pages 217–239. Springer, 2014.

[13] I. Haitner and E. Tsfadia. An almost-optimally fair three-party coin-flipping protocol. In *Proceedings of the 46th Annual ACM Symposium on Theory of Computing (STOC)*, pages 817–836, 2014.

[14] I. Haitner and E. Tsfadia. An almost-optimally fair three-party coin-flipping protocol. *SIAM J. Comput.*, 46(2):479–542, 2017.

[15] I. Haitner, K. Nissim, E. Omri, R. Shaltiel, and J. Silbak. Computational two-party correlation. Unpublished manuscript, 2018.

[16] R. Impagliazzo and M. Luby. One-way functions are essential for complexity based cryptography. In *Proceedings of the 30th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 230–235, 1989.

[17] T. Moran, M. Naor, and G. Segev. An optimally fair coin toss. In *Proceedings of the 6th Theory of Cryptography Conference, TCC 2009*, pages 1–18, 2009.

[18] T. Moran, M. Naor, and G. Segev. An optimally fair coin toss. *Journal of Cryptology*, 29(3): 491–513, 2016.